新興浪潮：危及公共建設安全的最新駭客攻擊

TrendLabs℠ 2015 年第二季資訊安全總評

趨勢科技法律免責聲明

本文之內容僅供一般資訊及教育用途。不作為也不應視為法律諮詢建議。本文之內容可能不適用於所有情況，也可能未反映出最新的情勢。在未就特定事實或所呈現之情況而徵詢法律建議之前，不應直接採信本文之所有內容或採取行動。趨勢科技保留隨時修改本文內容而不事先知會之權利。

所有翻譯成其他語言之內容僅供閱讀之方便。翻譯之準確性無法保證。若有任何關於翻譯準確性的問題，請參考本文件原始語言的官方版本。任何翻譯上的不一致與差異皆不具約束力，且在法規與執法上不具法律效力。

儘管趨勢科技已盡合理之努力確保本文內容之準確性與時效性，但趨勢科技對其準確性、時效性與完整性不提供任何擔保或聲明。在您存取、使用及採納這份文件內容時，即同意自行承擔任何風險。趨勢科技不提供任何形態之擔保，不論明示或隱含之擔保。趨勢科技或建立、製作或供應此文件之任何相關對象，對於存取、使用、無法使用、因使用本文、因本文內容之錯誤或遺漏而引起之任何後果、損失、傷害皆不承擔責任，包括直接、間接、特殊、連帶、營利損失或特殊損害賠償。使用本文之資訊即代表接受本文之「原貌」。

內容

4

最新駭客攻擊造成公共建設停擺

7

全球各地出現網路犯罪個體戶，而勒索軟體和 PoS 惡意程式也持續肆虐

14

資安獲得政府重視，執法機關大有斬獲

17

全國性衝擊與政治效應：美國人事管理局 (OPM) 資料外洩如何成為有史以來最大的一樁資料外洩事件

20

政府機構遭到最新攻擊，突顯進階持續性滲透攻擊 (APT) 的政治意圖

24

系統漏洞威脅公共網站與行動裝置

26

Angler 漏洞攻擊套件連線數量翻了三倍，收錄最新漏洞的速度加快

31

威脅情勢回顧

這已不再是科幻情節：民航客機遭到攻擊、家用路由器遭到挾持、電視廣播網路遭到關閉。本季的資安事件顯示駭客正絞盡腦汁尋找更令人意想不到的方法來滲透並操控我們的日常科技。過去我們已見過類似的攻擊，但其影響層面和今日真是不可同日而語。過去，網路犯罪集團都是以竊取資料和財物為主。駭客攻擊大型企業或機構，目的是為了獲得更高的報酬。隨著越來越多公共建設開始連上網路，我們發現一些昔日的攻擊手法有死灰復燃的現象，而且衝擊比以往更大。

駭客正在尋找新的方法來攻擊一些人們通常不會防備的生活科技。他們已找到一些操控家用路由器並侵犯使用者隱私的方法。此外，銷售櫃台系統 (PoS) 惡意程式的日益精進，也讓越來越多企業蒙受營業損失。駭客不斷在測試軟體和系統的漏洞，並為其發現的漏洞尋找適當的用途。從交通運輸安全相關的研究數量不斷增加即可看出，駭客攻擊未來很可能變成一項更常見、更具體的安全威脅。例如，航空公司班機遭駭將帶來嚴重的飛安問題。未來萬一歹徒看上智慧型大眾運輸工具會是甚麼樣的情況？

這一切並非表示網路犯罪集團已開始放棄他們舊的營運模式。傳統惡意程式仍是他們現行的主要工具，這一點從它們在全球一些特定區域非常活躍即可證明。由於一些基本的惡意程式元件和工具如此唾手可得又容易使用，因此，任何新手都能在網路犯罪市場闖出一番事業。

儘管執法機關正快馬加鞭迎頭趕上，例如 Silk Road (絲路) 地下市集幕後首腦 Ross Ulbricht 遭到起訴即是一項重要指標，但資訊安全仍有許多尚待努力之處。隨著資訊科技不斷向前邁進，未來勢必將會出現一波波新的資安挑戰。不僅如此，由於資訊科技越來越普及到大眾的日常生活當中，人們也將更容易感受到資安威脅所帶來的衝擊。

註：文中所有提到「偵測」一詞的之處，皆指趨勢科技安全防護產品在使用者裝置上發現並攔截到的威脅。除非另有說明，否則本報告當中的數字皆來自趨勢科技 Smart Protection Network™ 雲端防護基礎架構所蒐集之資料。該基礎架構結合了雲端與用戶端技術來支援企業內安裝的產品以及雲端代管式服務。

最新駭客攻擊造成公共建設停擺

家用路由器遭駭、大型電視網路遭到駭客激進份子全面攻擊，甚至有民航客機遭到駭客入侵。若我們能從本季記取什麼教訓，那就是：網路威脅真的存在。

一位知名的飛航安全研究員 Chris Roberts 今年五月登上新聞頭條，他被控駭入飛機上的艙內娛樂系統。根據美國聯邦調查局 (FBI) 的報告，Roberts 造成「飛機的其中一個引擎轉速攀升，導致飛機橫向平移。」[1、2] Roberts 今年四月才遭到美國聯合航空 (United Airlines) 一架班機驅逐，原因是他在推特上發文談論飛機的安全漏洞，後續更引起進一步有關艙內網路是否可能遭到駭入的調查。[3] 今年六月，一項針對波蘭國家航空網路的攻擊登上新聞，有數十架班機遭停飛數個小時，超過 1,400 名旅客受到影響。[4]

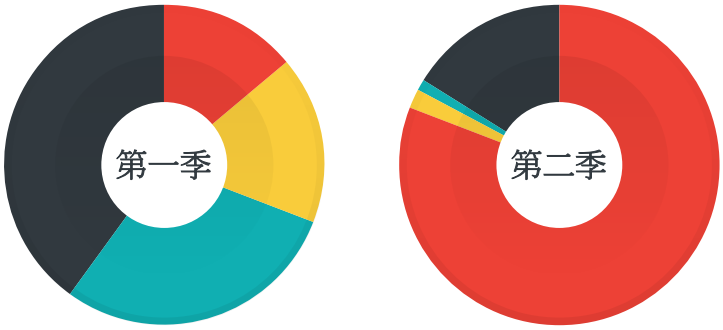
根據我們的研究，只要有適當的工具，再加上一些天分，要入侵自動化運輸系統是一件輕而易舉的事。2014 年第四季，我們討論了有關「船舶自動辨識系統」(Automatic Identification System，簡稱 AIS) 的漏洞，這是用來追蹤海上船隻動態的一套系統，我們提出駭客可能如何偽造船舶航行數據來製造恐慌或造成災難。此外，我們研究人員對智慧型車輛的研究也證實，駭客可能入侵私人交通運輸工具。

不僅如此，我們也研究了本季多起針對家用路由器的攻擊。藉由篡改網域名稱系統 (Domain Name System，簡稱 DNS) 的攻擊，早已不是新聞，只不過，修改 DNS 來攻擊家用路由器的手法似乎又開始死灰復燃。本季，網路犯罪集團盯上了家用路由器，藉由篡改這些裝置傳輸給連接裝置的資訊來幫助他們竊取資料。[5]

惡意程式會感染路由器並修改其 DNS 設定，進而讓網路犯罪集團從事惡意活動，例如將受害者重導至惡意網站。這些惡意網站有些是網路釣魚網站，有些則是專門散布惡意程式的冒牌網站。

我們發現 DNS 篡改程式的偵測數量在巴西有增加的趨勢。[6] 這些惡意程式會試圖掌控路由器並修改其 DNS 設定。

DNS 篡改程式偵測數量 (2015 年第一季和第二季)



	第一季	第二季
巴西	14%	81%
美國	17%	2%
西班牙	29%	1%
其他	40%	16%

本季巴西囊括了全球所有 DNS 篡改程式偵測數量的 81%，遠遠超越上一季的 14%。

針對家用路由器的攻擊數量已暴增到了令人擔憂的程度，因為這些裝置在家用網路扮演了關鍵的角色。隨著越來越多裝置連上家用路由器，這些路由器就越容易成為駭客攻擊的目標。畢竟，一旦駭客滲透了含有漏洞的路由器，就能看到所有連上路由器的裝置，甚至取得路由器傳遞的所有資訊。

過去我們已見過 DNS 篡改程式可毒化搜尋結果或者修改路由器設定來將受害者重導至惡意網頁。連上已感染路由器的裝置越多，可能遭到詐騙的受害者就越多。

有別於傳統網路犯罪攻擊的影響表面上不太看得出來，本季駭客攻擊的效果則顯得相當明顯而真實。舉例來說，法國電視台 TV5MONDE 的廣播訊號及內部網路即因駭客攻擊而中斷了四小時之久。[7] 其網站和社群媒體帳號也無法倖免。

> 如同任何其他系統一樣，這套[艙內]系統也存在著漏洞，沒有任何人類創造的系統是 100% 沒有錯誤的。因此，政府和監理機關必須強制飛機和艙內娛樂系統製造商不能只想單靠資訊不透明來達到安全性，而是應該證明現有系統的安全性，並且修正任何已經曝光的漏洞。誰知道呢？說不定現有的系統設計就已經夠安全了，能夠抵擋駭客的攻擊。
>
> **—Martin Rösler**
>
> *威脅研究資深總監*

全球各地出現網路犯罪個體戶，而勒索軟體和 PoS 惡意程式也持續肆虐

本季，我們見到網路犯罪個體戶利用惡意程式來散播災難，例如 FighterPOS。此外，一位名叫「Lordfenix」的巴西駭客也是其中之一。而專門販賣竊取資料的加拿大駭客「Frapstar」同樣也是一位網路犯罪個體戶。

網路犯罪駭客總是不斷在更新其惡意程式碼，這一季也同樣如此。畢竟，修改現有惡意程式來發動新的攻擊是最快的方法。不但如此，任何人只要具備一些基本的工具和知識就能辦到，即使是個人。

例如，HawkEye 鍵盤側錄程式背後就是兩名網路犯罪個體戶。他們都使用一般很普通的資料竊取惡意程式來攔截企業的交易，專門鎖定中小企業 (SMB) 下手。[8] 他們會重新修改現有的惡意程式、工具套件和技巧來攻擊印度、埃及、伊朗、巴基斯坦、台灣以及美國等地的受害者。

HawkEye 受害者分布國家 (2015 年第二季)

受 HawkEye 危害最嚴重的產業 (2015 年第二季)

設備	18%
運輸	16%
製造	8%
醫療器材	6%
採礦	6%
營造	4%
重工業	4%
旅館	4%
廣告	2%
建築	2%
其他	30%

HawkEye 的受害者大多是中小企業，廣泛分布各種產業。

歹徒經常會修改一些傳統的惡意程式，如簡單的鍵盤側錄程式，來配合其攻擊對象。然而惡意程式的散布手法，則隨其活動的地點而異。

例如 Frapstar 是一位加拿大的網路犯罪個體戶，其大部分的收入來自販售其竊取到的資訊。[9] 另一位 20 歲的巴西大學生 Lordfenix 則是靠販賣銀行惡意程式賺錢。[10] 根據我們的研究發現，Lordfenix 從 2013 年 4 月至今已開發了超過 100 個銀行木馬程式，每一個價格約在 1,000 巴西幣 (約 320 美元) 左右。至於 Frapstar 則在一些已知的網路犯罪和駭客論壇上非常活躍，兩者都是非法敏感資料常見的交易平台。

今年四月出現的 FighterPOS 惡意程式背後同樣是一名網路犯罪個體戶。FighterPOS 感染了 100 台以上的 PoS 終端機，並從中竊取了大約 22,000 個非重複的信用卡卡號，活動範圍主在巴西 (96%)。[11] 不僅如此，FighterPOS 的作者似乎長期從事信用卡資料竊取、付款詐騙、惡意程式開發等非法工作。

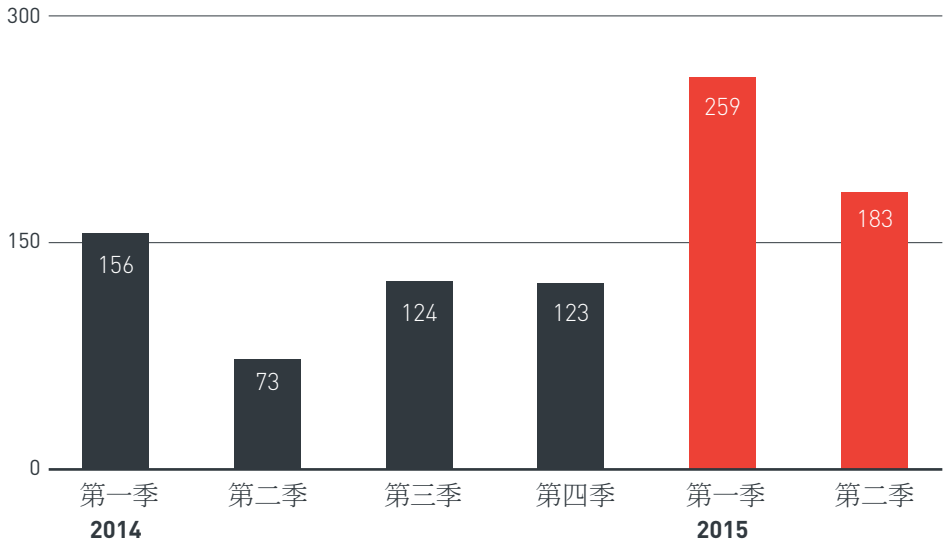
今年六月新發現的 MalumPOS 惡意程式專門鎖定採用 Oracle® MICROS 平台的系統，大約感染了 330,000 個旅館、餐飲、零售等產業的據點，主要分布於美國。隨著 PoS 惡意程式的變種越來越多，遲早會有其他有心的網路犯罪份子修改其原始程式碼來做其他用途。

網路犯罪集團/幕後首腦 (2015 年第二季)

集團/幕後首腦	受害國家
HawkEye	印度、埃及、伊朗、巴基斯坦、台灣、美國、香港、俄羅斯、法國、德國
Lordfenix	巴西
Frapstar	美國、加拿大*
開發行動勒索軟體的中國青年	中國
TorrentLocker	澳洲、西班牙、德國、法國、英國、土耳其、波蘭、美國、義大利、台灣、紐西蘭、荷蘭
CryptoWall 3.0	美國、加拿大、印度、英國、法國、日本、台灣、南韓、澳洲

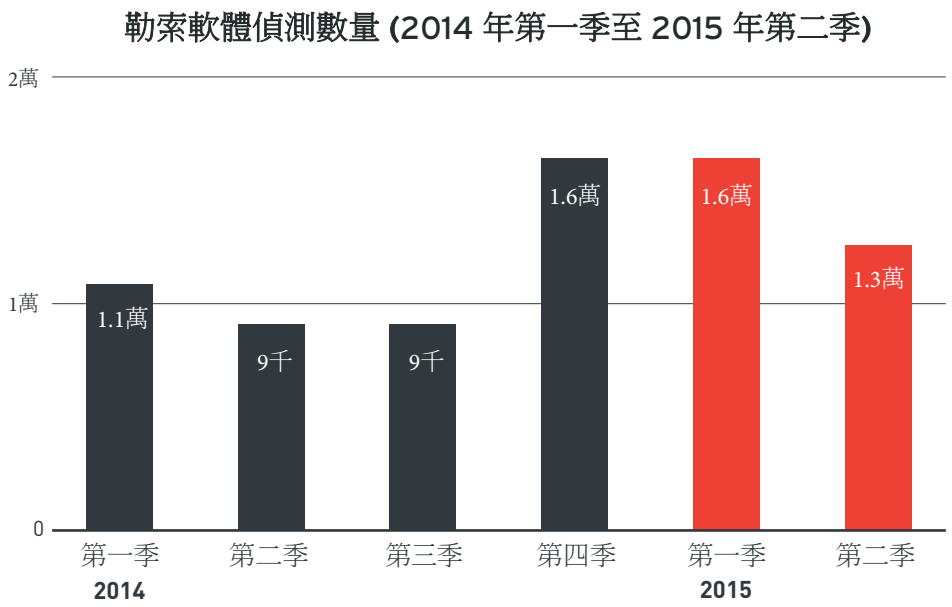
**註：Frapstar 有可能也在表中所列以外國家販售其資訊。*

PoS 惡意程式偵測數量 (2014 年第一季至 2015 年第二季)



本季 PoS 惡意程式偵測數量稍微下降，有可能是威脅的數量已經到達飽和。今年上半年最後一輪威脅，或許是歹徒最後的奮力一搏。

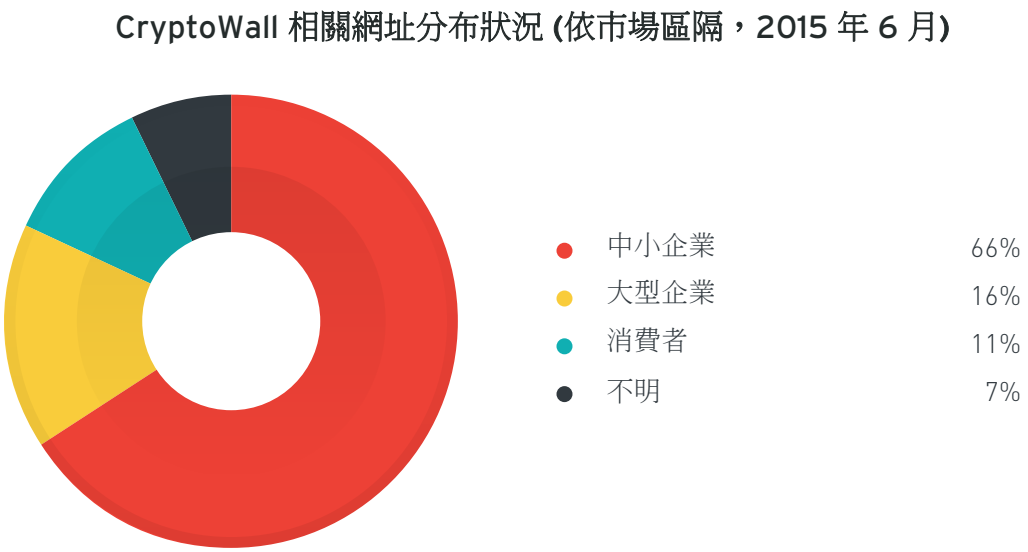
勒索軟體偵測數量或許看來好像開始走向下坡，但經過深入分析之後，這些威脅短期內並無消失的跡象，只是越來越朝區域化發展而已。



自從 2015 年第一季之後，勒索軟體的偵測數量即開始走向下坡。

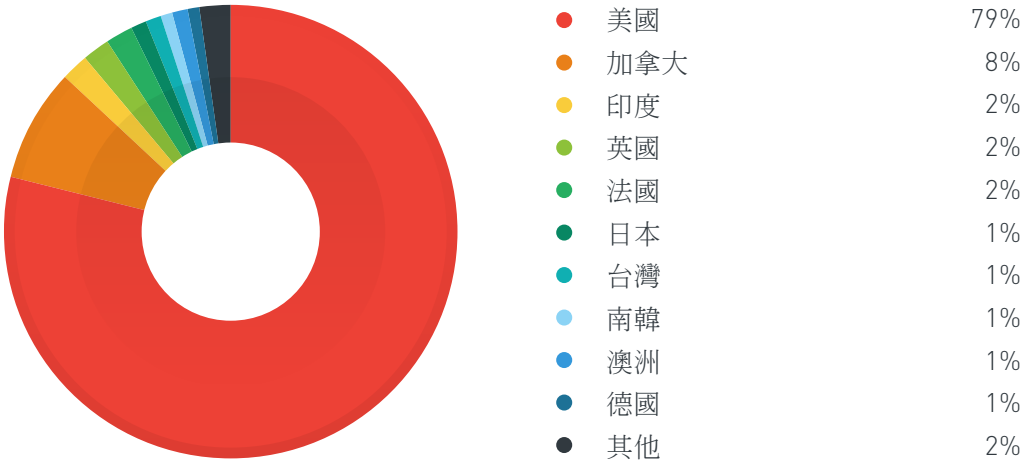
我們應該從各種不同的角度來分析勒索軟體所帶來的風險。感染電腦只不過是它們的其中一項能力。就在今年六月，我們密切監控了兩個知名的勒索軟體變種：CryptoWall 和 TorrentLocker。

CryptoWall 3.0 是這個加密勒索軟體的最新變種，專門經由垃圾郵件散布，甚至曾經和 FAREIT 同夥。[12]



根據 2015 年 6 月蒐集到的資料，受 CryptoWall 危害最嚴重的是中小企業。

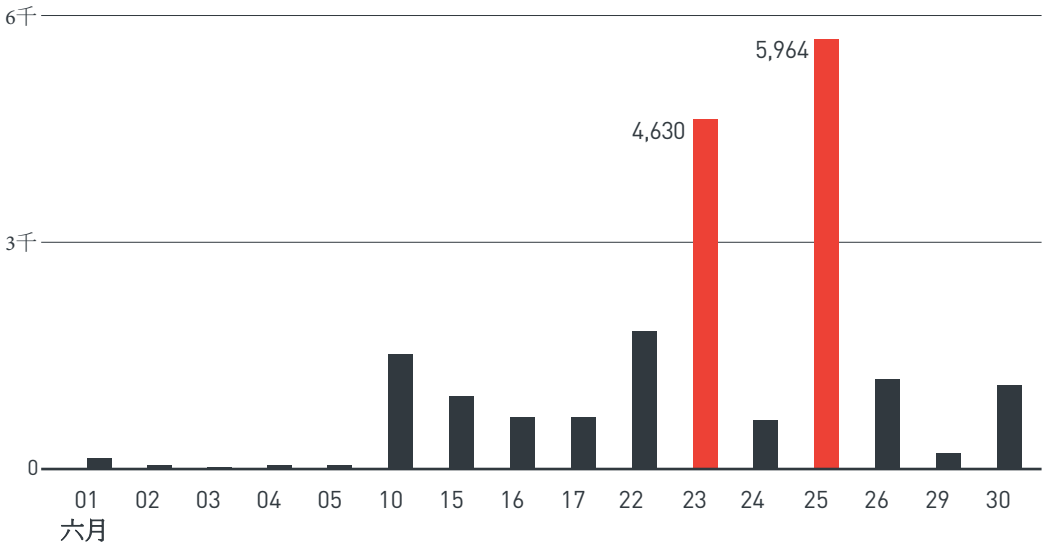
CryptoWall 受害者分布十大國家 (2015 年 6 月)



CryptoWall 絕大部分的受害者都分布在美國，幾乎占了偵測總數的 80%。

光是今年六月，使用者就存取了超過 10,000 個 TorrentLocker 相關網址。尤其是 6 月 23 日和 25 日，使用者一天內存取的數量就超過 4,000 個以上。這表示點選電子郵件內連結的使用者越來越多，同時也突顯架設一套多層式防護對於防範勒索軟體的重要性。

點選 TorrentLocker 散布網站連結的使用者數量 (2015 年 6 月)



光是今年六月，我們就攔截了超過 10,000 個使用者點選的 TorrentLocker 相關網址，尤以該月 23 和 25 日攔截到的數量最高。

各地區爆發勒索軟體攻擊的情況 (2015 年 6 月)

從月曆當中我們可看出歹徒有計畫地在特定國家散布勒索軟體，包括 TorrentLocker 和 CryptoWall 變種。

本季，我們也看到散布 TorrentLocker 相關網址的電子郵件大量集中在某些國家，尤其是英國和土耳其。[13] 這些電子郵件經常假冒知名郵務、快遞機構和電信業者 (如 SDA Express、Pozcta、Correo 以及 Turkcell) 的名義為社交工程誘餌。不過近期的變種已經開始改變其惡意程式存放的網站。它們不再喜歡 SendSpace 和 Mediafire，而是改用 Yandex Disk 和 Google Drive™ 為存放地點。

行動勒索軟體在中國也同樣橫行，但背後的犯罪集團卻令人出乎意料。根據我們對地下市場的研究指出，目前某個 Android™ 勒索軟體已有上千個變種。在仔細研究過這些變種之後可以看出，它們全都來自同一份原始碼，而這份原始碼在地下市場流通相當廣泛。該原始碼是由一群新一代網路犯罪集團所開發，年齡在 16 至 21 歲之間。[14] 他們似乎更大膽、更肆無忌憚，甚至在網路上留下自己的真實身分。他們甚至為一些想要從事網路犯罪的新手提供教學服務。而且有別於經驗豐富的老手，這些新生代偏愛透過支付寶、微信以及銀行轉帳來接受付款，完全與當今透過數位貨幣來避免遭到追查的犯罪潮流背道而馳。

> 未來，我們或許會看到新舊威脅融合為一體，為了相同的目的而結合。防禦的一方，必須開始思考這些最新的未來威脅，同時還要應付舊式威脅，並且隨時提防潛在的進階持續性滲透攻擊 (APT)。我會建議務必採用一套清楚明確的策略來對抗這些威脅。除了追查個別主機上的特定事件之外，還要能夠掌握它們與網路事件之間的關聯。
>
> **—Jay Yaneza**
>
> *威脅分析師*

資安獲得政府重視，執法機關大有斬獲

本季我們看到更多的聯合執法行動，並接連破獲多個殭屍網路，逮捕了一些網路犯罪份子，產生了實質的效應。但這只不過證明了一件事：對世界真正有影響的網路犯罪，其效果是非常具體的。

當今值得我們注意的一項發展就是執法機關與民間企業之間的密切合作。趨勢科技協助執法機關破獲了兩個惡名昭彰、嚴重涉及大規模網路犯罪的殭屍網路：SIMDA 和 Beebone。

在一項公私部門合作 (PPP) 當中，趨勢科技、美國聯邦調查局 (FBI)、歐洲刑警組織 (Europol)、美國國土安全部 (DHS) 以及其他資安廠商，在今年四月共同破獲了一個經營已久的 Beebone 殭屍網路。[15、16] Beebone 惡意程式 (也就是我們偵測到的 VOBFUS 變種) 是具備變形能力的惡意程式，專門用來下載其他惡意程式。[17]

同月，另一項聯合行動亦傳來捷報，破獲了 SIMDA 殭屍網路，參與這次行動的有趨勢科技、國際刑警組織 (INTERPOL)、Microsoft、Kaspersky，還有日本的網路防禦研究所 (Cyber Defense Institute)，這又是資安產業的一大勝利。[18] 研究人員認為 SIMDA 殭屍網路的活動範圍遍及全球，重新導向伺服器遍布 14 個國家，受害者至少分布 62 個國家。[19]

深入深層全球網路 (Deep Web)

今年二月，聯邦檢察官正式起訴了 Silk Road (絲路) 地下市集首腦：現年 31 歲的 Ross Ulbricht。[20] 幾個月之後，在今年五月，Ulbricht 被判終身監禁，不得假釋。[21] Silk Road 曾經是全球最大的黑暗全球網路 (Dark Web) 市集，專門販賣毒品，而且能確保使用者的私密性和匿名性。

Ulbricht 遭到判刑，讓原本深邃而神秘的深層全球網路 (Deep Web) 以及其他相關犯罪活動因而曝光。在為期兩年的過程中，趨勢科技前瞻威脅研究 (Forward-Looking Threat Research，簡稱 FTR) 團隊深入

探索深層全球網路的秘密以及對真實世界的影響。[22] 我們在幾個月前發表的研究報告顯示，深層全球網路上販賣的最大宗商品正是毒品。不僅如此，深層全球網路還是許多網路犯罪集團從事比特幣 (Bitcoin) 交易和洗錢的大本營。

Ulbricht 的判刑等於是給所有想要有樣學樣的人一個清楚的警告。目前我們還未看到網路犯罪地下市場有任何劇烈的變動，但由於像 Ulbricht 這類歹徒都是在深層全球網路當中行動 (而這正是執法上的一大挑戰)，因此我們應該花更多功夫來調查這個黑暗網路。

深層全球網路上販賣的產品與服務現況 (2015 年第二季)

項目	價格
帳戶餘額至少 500 美元的德國 PayPal 帳號	250 美元
100 個尚未確認的 PayPal 帳號	100 美元
100 個尚未確認的 eBay 帳號	100 美元
100 個未經確認的信用卡卡號及 CVV2 驗證碼	150 美元
偽造歐洲護照	500–750 歐元
偽造美國護照	800 歐元
帳單餘額 2,000 美元的美國信用卡	90 美元
帳單餘額 5,000 歐元的歐洲信用卡	210 美元

資料來源：

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf

在隱私權和安全之間求取平衡

本季破獲殭屍網路和逮捕網路犯罪集團的行動，證明資訊安全是美國政府的一項優先要務。美國政府才在今年六月通過了最新的「美國自由法」(USA Freedom Act)，目的就是要讓人民能夠自由地使用通訊科技，同時限制情報單位的資料蒐集行動。[23] 此外，美國更大膽地採取一項安全措施，規定所有聯邦政府網站都必須採用 HTTPS 加密通訊協定，以確保所有網站瀏覽者的安全和私密性。[24] 雖然這並不足以解決所有的網路威脅，但這絕對是一項正面的改革。

同月，歐盟理事會 (Council of the European Union) 同意通過新的歐洲資料保護法，希望能讓較嚴格的新法規得以在整個歐盟區實施。[25]

“

網路犯罪讓立法機關最頭痛的問題就是他們演進的速度太快。大部分的法律都需要 3 到 5 年才能通過。因此，最重要的就是一些存在已久的通用法律。美國在打擊組織犯罪與勒索詐騙方面做得相當成功。儘管這些法律不是針對「網路犯罪」而設，但依然能發揮一定的作用。基本上我們該做的就是讓不同國家之間的法律一致。

網路無國界，網路犯罪是全球性的。因此，如果駭入伺服器這項網路犯罪的法律規定在德國、冰島或法國都一致，那麼要起訴罪犯就容易許多。而且當發生這類案件時，也不會像現在這麼複雜。最重要的是，能讓公私部門之間的合作溝通更順暢。只要溝通順暢，執法機關和資安研究人員就能輕鬆分享情報。

”

—Robert McArdle

資深威脅研究經理

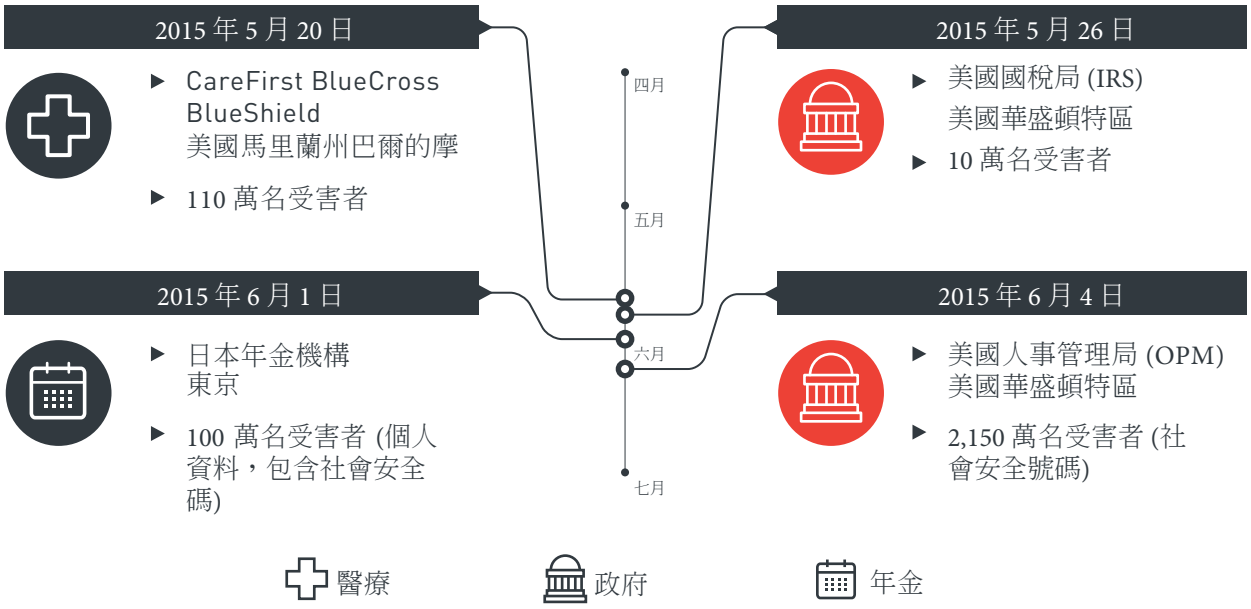
全國性衝擊與政治效應：美國人事管理局 (OPM) 資料外洩如何成為有史以來最大的一樁資料外洩事件

今年六月下旬，美國政府宣布將對人事管理局 (OPM) 系統發生的大規模資料外洩事件展開調查。[26] OPM 隸屬於美國聯邦人力資源部，負責執行所有州政府員工的背景調查。據估計，大約有 2,100 萬名前任和現任聯邦政府員工 (包括被否決的應徵者) 個人資料因而曝光。[27]

駭客所選擇的攻擊目標並不稀奇。我們已經知道，人事部門經常是跳島式 (或蛙跳式) 攻擊的第一波目標，但歹徒「真正」的目標，是該部門的相關單位。[28] 歹徒所竊取的資料數量之多，已經足以引起嚴重的擔憂，再加上外洩資料之完整，這次事件的衝擊絕對是毫無疑問的。駭客已取得了數百萬份美國國家安全職務表格 (SF-86 表格) 的資料。這些資料當中包含了社會安全碼 (如同身分證字號)、工作職務、應徵者的背景與親朋好友等資訊。根據報導，外洩的資料還包含針對聯邦政府員工和約聘人員的安全背景調查，這些很容易遭歹徒用於身分冒用、詐騙和網路釣魚。更嚴重的一項後果是，這些外洩的資訊很可能造成國家安全威脅。[29]

不僅如此，美國國稅局 (IRS) 也同樣發生資料外洩，駭客在今年五月從國稅局的「Get Transcript」網站竊取了一些資料。在該案當中，駭客取得了 100,000 多名納稅人的資料，包括：社會安全碼、出生日期與住家地址。[30、31] 今年六月，日本年金機構 (Japan Pension Service) 也因員工開啟了一封惡意郵件附檔而引狼入室，導致資料外洩。[32]

已曝光的重大資料外洩 (2015 年第二季)



政府機關是本季的主要攻擊目標。OPM 資料外洩是有史以來最大的一樁外洩事件，超過 2,000 萬筆資料遭到曝光。

資料來源：https://www.privacyrights.org/data-breach

> 在某些方面，您的個人資訊遭到外洩其實更加危險。我可以輕易更換一張信用卡，但除非我搬家，否則我的住址不能變更。出生日期也無法改變。個人身分識別資訊 (PII) 不僅能用來識別身分，而且通常很難改變 (就算並非不可能)。

—Raimund Genes

技術長

政府機構遭到最新攻擊，突顯進階持續性滲透攻擊 (APT) 的政治意圖

我們看到 Pawn Storm 攻擊行動的駭客過去曾攻擊北大西洋公約組織 (NATO) 會員國及美國白宮。此外，ESILE (或稱 Lotus Blossom) 以及 Tropic Trooper 等攻擊行動，則是專門鎖定東南亞國家政府機關。根據我們 Smart Protection Network 的資料，駭客正在尋找更多利用巨集惡意程式的機會，發動以政治為意圖的攻擊。

本季出現的攻擊行動：Pawn Storm、ESILE/Lotus Blossom、Tropic Trooper 與 DUQU 2.0

今年四月，趨勢科技研究人員發現 Pawn Storm 涉及一些新的攻擊行動，專門鎖定北約 (NATO) 會員國和美國白宮。Pawn Storm 駭客會散布精心製作的電子郵件，來誘騙受害目標點選惡意連結。他們會在政府機關網站上植入惡意程式，並透過新的幕後操縱 (C&C) 伺服器來攻擊北約會員國以及歐洲、亞洲、中東的政府機關。[33]

今年五月，Tropic Trooper 攻擊行動 (依歹徒選擇的目標而命名) 專門攻擊台灣和菲律賓的政府機關。[34] 該行動使用的是舊式滲透技巧、兩個經常被攻擊的 Windows® 漏洞、一點基本的圖像隱碼術 (Steganography) 以及有效的社交工程。[35]

今年六月又有另一起 APT 攻擊行動登上新聞版面，那就是 ESILE (亦稱為 Lotus Blossom) 攻擊行動。據報導，這項行動在三年之內共發動了 50 起以上的攻擊，目標為東南亞的企業。[36] 根據我們的分析，該行動所使用的惡意程式會在系統植入一些精心製作、讓資安人員混淆的檔案。[37]

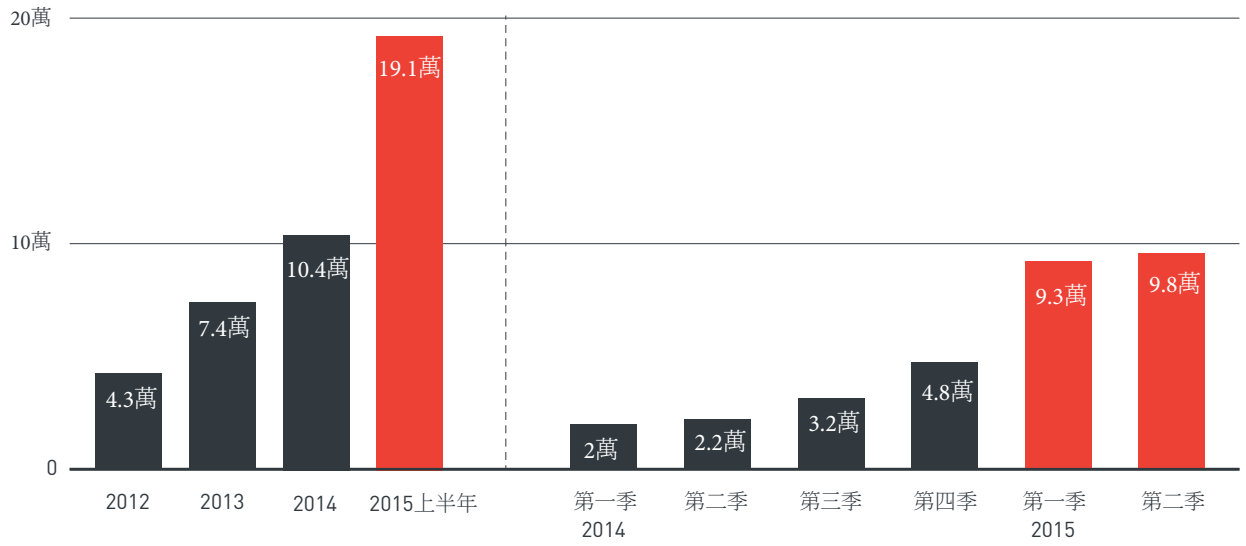
STUXNET 的後繼者：DUQU 首次在 2011 年 10 月登上新聞，當時研究人員發現兩者在程式碼上有諸多雷同。[38] 就在今年六月，我們發現了 DUQU 2.0 利用多個零時差漏洞來攻擊特定目標。[39] 資安研究人員相信，DUQU 2.0 與以色列有所關聯，而且是用來監視網路上有關伊朗核武能力的討論。[40]

APT 行動開始利用巨集惡意程式

巨集惡意程式除了被網路犯罪集團用於「一般傳統攻擊」之外，現在也開始受到 APT 的青睞。例如，Woolen-Goldfish 就利用魚叉式網路釣魚郵件來挾帶暗藏惡意巨集的 Microsoft™ Excel® 附件檔案。[41、42]

這些攻擊的存在，突顯了提升 APT 防範能力的重要性在今日更甚以往。因此，採用多層式的防護策略來對抗以電子郵件為媒介的攻擊有其必要，因為它們是 APT 最常用的攻擊管道。

巨集惡意程式偵測數量 (2012 年至 2015 年上半年)



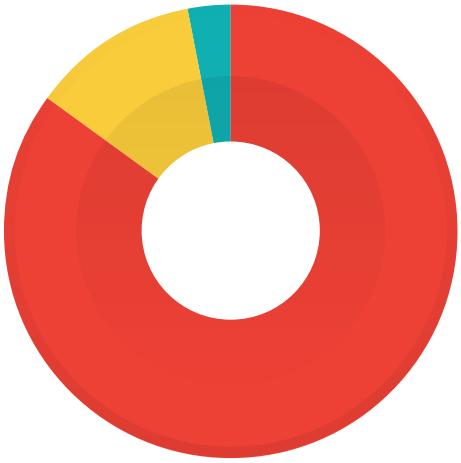
巨集惡意程式偵測數量較過去一季小幅增加，最可能的原因是連上巨集惡意程式下載網站的惡意廣告數量增加。

巨集惡意程式偵測數量最高的國家 (2015 年第二季)

中國	23%
美國	19%
英國	9%
日本	8%
法國	5%
澳洲	4%
台灣	3%
義大利	2%
印度	2%
德國	2%
其他	23%

今年第一季巨集惡意程式偵測數量最高的前四名國家，在第二季依然名列前茅。

各應用程式的巨集惡意程式偵測數量 (2015 年第二季)



Microsoft Word	85%
Microsoft Excel	12%
Microsoft PowerPoint, etc.	3%

本季絕大多數的巨集惡意程式都是透過 Microsoft Word® 文件散布。

“

傳統上，以政治為意圖的 APT 和以企業為目標的 APT 相當類似。不過，在動機和結果上，仍有一些微小差異。帶有政治意圖的攻擊，通常比較會使用零時差漏洞並搭配「傳統」攻擊管道。反觀針對企業的攻擊，大多都採用「標準」手法，因為歹徒幾乎都是仰賴「人」的成分，也就是最弱的安全環節。

”

—Kyle Wilhoit

資深威脅研究員

“

二次感染的情況越來越嚴重，主要是因為三個不利的現象所造成。第一，越來越多駭客開始鎖定企業的資訊供應鏈，利用跳島式攻擊來入侵內部主機。第二，在成功潛入之後，歹徒會利用一些圖像隱碼術 (Steganography) 在已入侵的系統上建立第二個 C&C 通訊管道，讓歹徒有效避開資安防護措施。最後，一旦歹徒竊取到智慧財產或個人身分識別資訊，就會冒用企業的名義，透過水坑式攻擊來襲擊其客戶。這樣的手法在 2015 上半年已呈現倍數成長。

”

—Tom Kellermann

網路安全長

系統漏洞威脅公共網站與行動裝置

本季告訴我們，網站應用程式的漏洞與那些使用者數量龐大的軟體漏洞一樣危險。

資安研究人員在一個專門處理銀行相關資訊的網站應用程式：Magento 當中發現了一個漏洞。[43] 根據報導，全球約有 20,000 個使用該平台的網站都有可能遭到惡意程式攻擊並造成信用卡盜用。Magento 是全球 240,000 多個網站背後的基礎，包括擁有 1 億 5 千 7 百萬活躍買家的全球知名電子商務網站 eBay 也是其中之一。不過 eBay 目前已解決了這個問題。[44]

今年四月，WordPress 的內容管理系統 (CMS) 遭到駭客攻擊，駭客在其瀏覽器介面的系統管理視窗上插入了惡意的 JavaScript 程式碼。[45] 這項由芬蘭研究人員 Jouko Pynnönen 所發現的漏洞能讓駭客利用以 WordPress 架設的論壇及討論區中的回應編輯方塊來發動跨網站腳本 (XSS) 攻擊，而這類網站卻大約占了全球網路的四分之一。

面對網站應用程式和軟體的漏洞威脅，行動裝置一樣無法倖免。例如，資安威脅人員宣稱全球 6 億支以上的 Samsung 行動裝置都存在著一個鍵盤漏洞。[46] 根據我們自己的分析，這個 Samsung SwiftKey 漏洞 (CVE-2015-4640 與 CVE-2015- 4641) 可讓潛在的駭客經由中間人 (MitM) 攻擊的手法在含有漏洞的裝置上執行惡意程式碼。[47、48、49] 儘管該漏洞已有修補程式，但由於系統更新不易，所以問題依然存在。使用者最終是否能夠收到更新，關鍵還是在於裝置廠商和電信業者。[50]

今年五月，Apache Cordova 應用程式架構在被發現一個漏洞。它讓駭客只要靠一個惡意網址就能修改應用程式的行為。[51] 這項高嚴重性的漏洞會影響絕大部分建立在 Cordova 平台的應用程式，占 Google Play™ 上所有應用程式的 5% 左右。此漏洞的編號為 CVE-2015-1835，可能造成裝置上的應用程式當掉。[52]

今年六月，Mac OS® X 出現可能波及 iOS 裝置使用者的漏洞。原本應該負責「保護」這兩個平台的應用程式沙盒環境被發現巨大漏洞。此漏洞可能讓駭客製作出可竊取鑰匙圈和 1Password 帳密管理軟體資料的應用程式。[53]

“

駭客對任何平台的漏洞都不會放過，他們就是一心想要找到滲透的管道。企業對於自己所使用的一些核心軟體與外掛程式的漏洞要非常小心。除了實施持續的漏洞評估計畫之外，更需搭配組態管理計畫。雖然一般來說，我們都是以 Flash、Java、Firefox、Internet Explorer® 等常見的標準軟體來衡量當前的威脅情勢，但我們也別忘了一些客製化應用程式 (主要為網站應用程式) 的漏洞數量同樣非常驚人，而且很多並未收錄在 CVE 漏洞名單當中。客製化的程式需要客製化的檢查方法。針對客製化應用程式進行一番徹底的滲透測試，絕對是值得的。

”

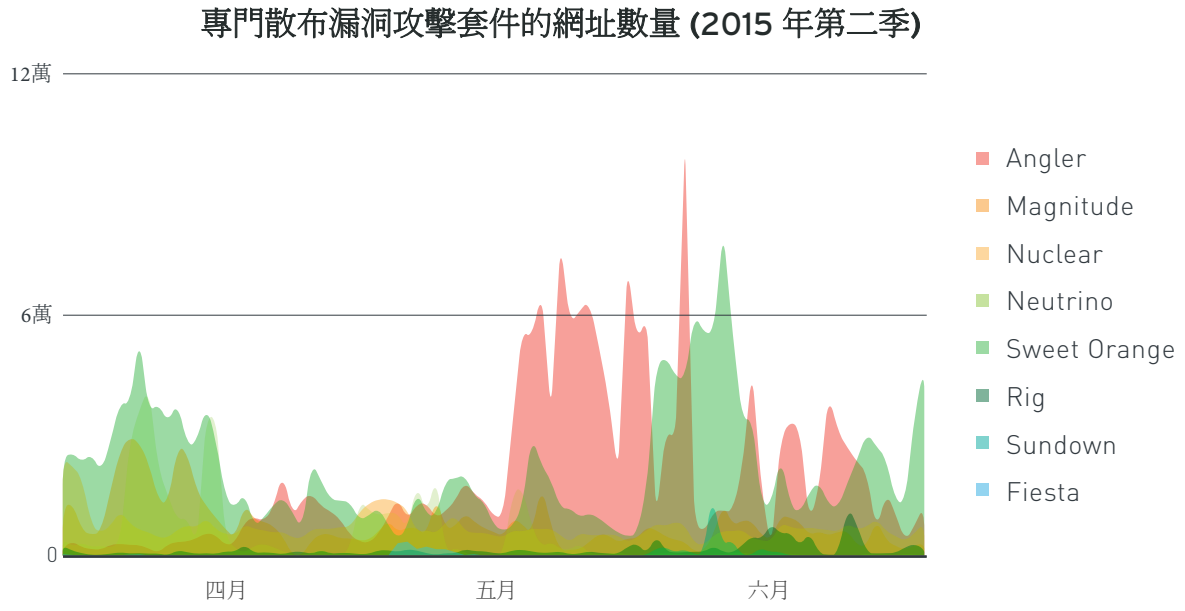
—Pawan Kinger

Deep Security Labs 總監

Angler 漏洞攻擊套件連線數量翻了三倍，收錄最新漏洞的速度加快

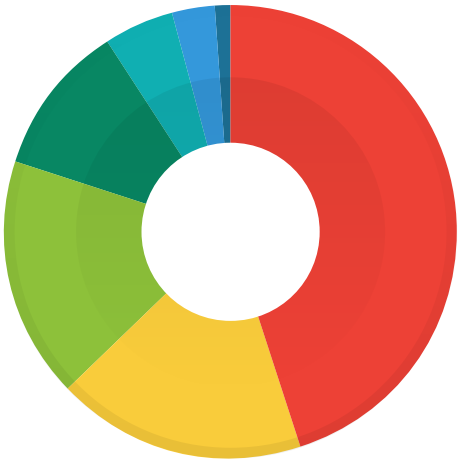
我們看到漏洞攻擊套件相關惡意程式偵測數量較上一季成長 67%。Angler 漏洞攻擊套件的數量翻了三倍，其作者已迅速將一些最新曝光的 Adobe® Flash® 漏洞收錄到該套件當中。

如同 Angler 漏洞攻擊套件一樣，Magnitude 和 Nuclear 兩個漏洞攻擊套件也經常成為 Adobe Flash 漏洞攻擊的常客。



使用者存取 Angler 漏洞攻擊套件散布網站的數量從今年五月份開始飆高，一直持續到六月初。在這期間，專門顯示惡意廣告的已入侵網站及成人網站數量也同樣增加，而這些廣告會將使用者導向專門散布 Angler 漏洞攻擊套件的網站。

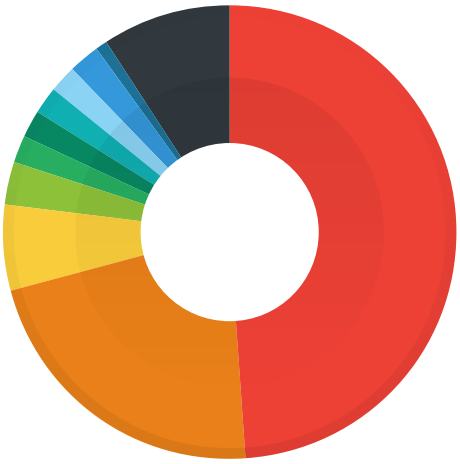
漏洞攻擊套件相關網址存取數量分布 (2015 年第二季)



Angler	45%
Magnitude	18%
Nuclear	17%
Neutrino	11%
Sweet Orange	5%
Rig	3%
Sundown	1%

Angler 漏洞攻擊套件在本季取代了 Nuclear 漏洞攻擊套件的地位，使用者存取其相關網址的數量明顯領先。

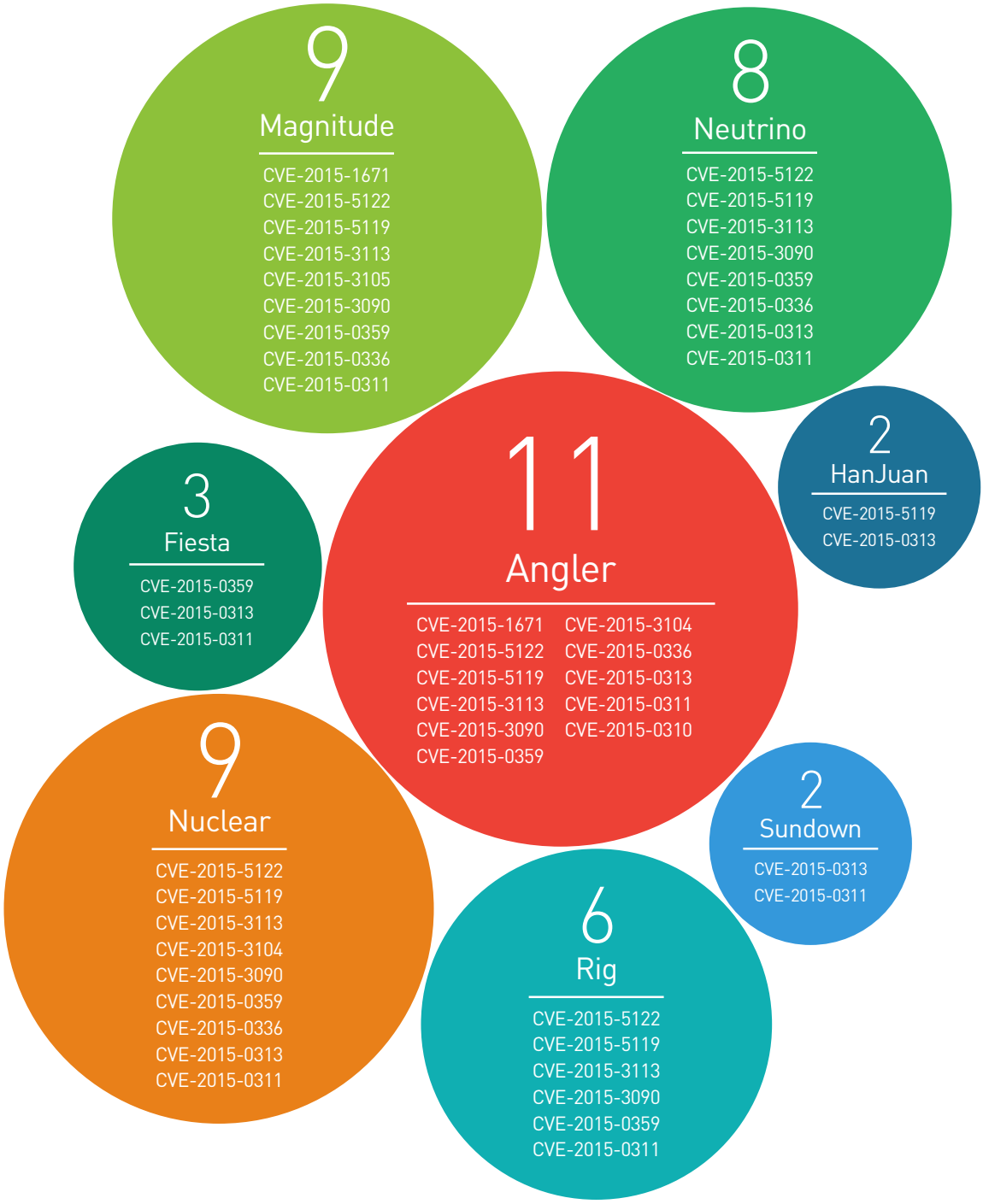
受 Angler 漏洞攻擊套件危害最嚴重國家 (2015 年第二季)



日本	49%
美國	22%
澳洲	6%
加拿大	3%
泰國	2%
法國	2%
丹麥	2%
英國	2%
台灣	2%
義大利	1%
其他	9%

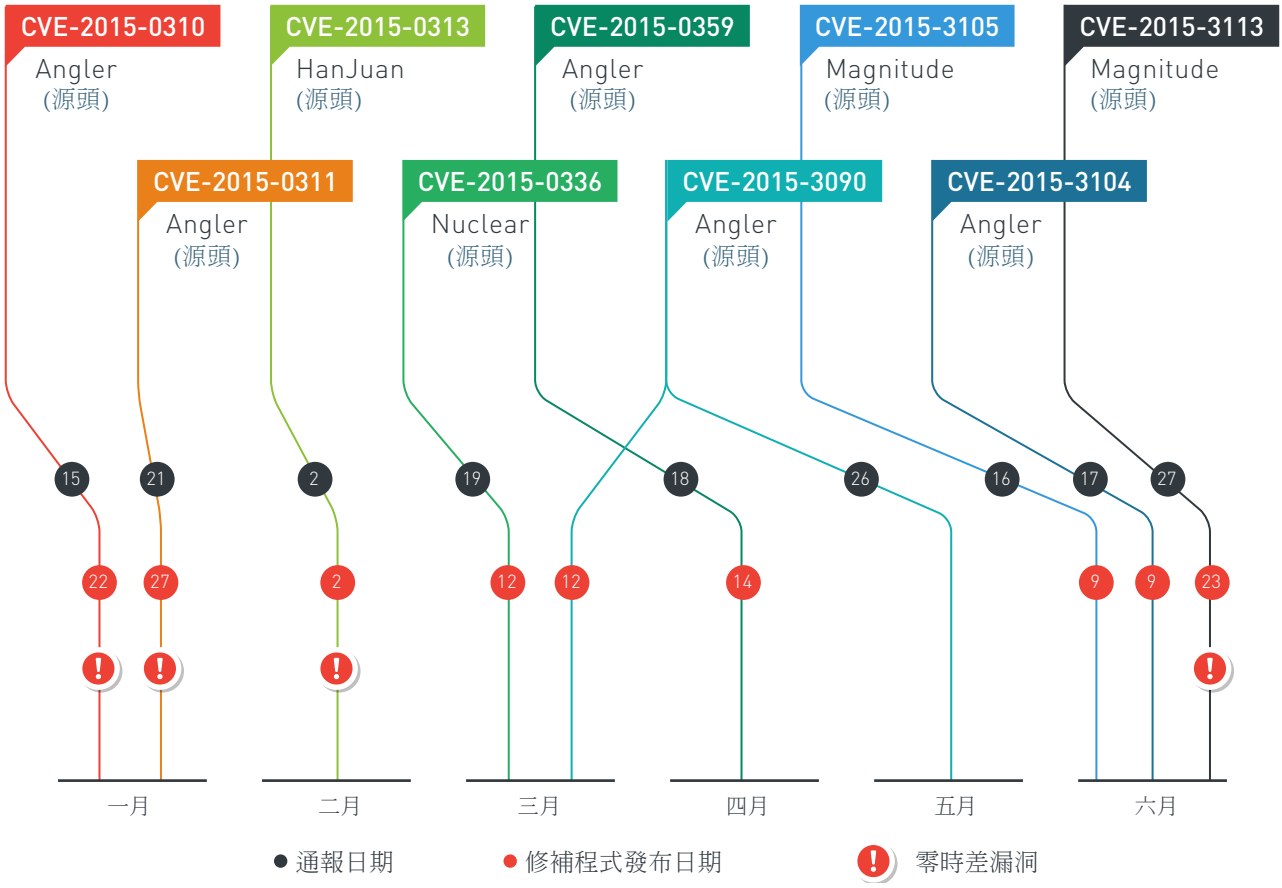
Angler 漏洞攻擊套件相關活動的數量在日本突然飆高。事實上，日本是受害最嚴重的國家，其使用者存取相關網址的數量最多。

Angler 漏洞攻擊套件的作者顯然較其他套件的作者更多產、更有生產力，許多漏洞都已收錄在該套件當中。在該套件收錄的 11 項漏洞當中有 10 項是 Adobe Flash 漏洞，讓所有使用該軟體來播放內容 (例如影片) 的網站都處於危險。此外，Angler 和 Magnitude 漏洞攻擊套件還收錄了一個 Silverlight® 的漏洞 (CVE-2015-1671)。[54]



從今年初起，收錄 Adobe Flash 漏洞的攻擊套件越來越多 (特別是 Angler)。Angler 在四月、五月、六月都有持續更新。就在七月，資安研究人員 Kafeine 才指出 Angler 涉及了兩起零時差漏洞攻擊 (一起在 7 月 7 日，另一起在 7 月 11 日)。[55、56]

漏洞攻擊套件收錄 Adobe Flash 漏洞的時間表 (2015 上半年)



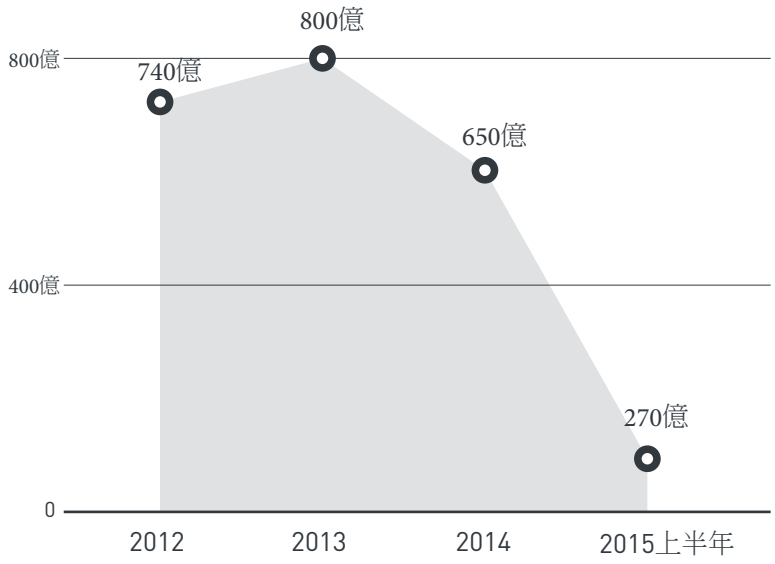
從今年初起，收錄 Adobe Flash 漏洞的攻擊套件越來越多 (特別是 Angler)。

> Angler 漏洞攻擊套件作者一直相當積極地主動收錄 Adobe Flash 漏洞。Magnitude 和 Nuclear 兩個套件的開發者也同樣如此。正因歹徒如此靈活，所以我們才要持續研究並監控最新的發展以保護我們的客戶。
>
> **—Joseph C. Chen**
> *威脅分析師*

威脅情勢回顧

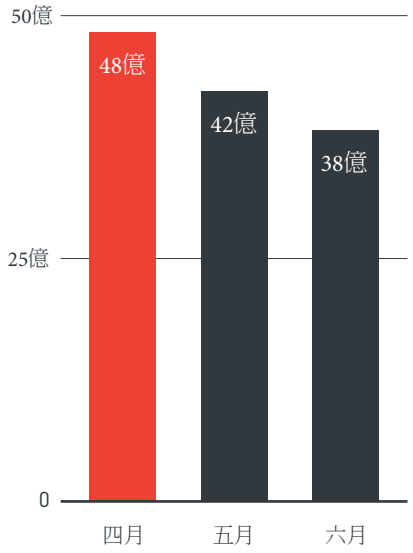
從 2012 年開始，我們 Smart Protection Network 全球威脅情報網路所蒐集到的數據整體上呈穩定下降的趨勢。這有可能意味著網路犯罪集團和駭客開始改變策略，不再採取「亂槍打鳥」的攻勢，因此不需大量的受害者來累積獲利。反而是聚焦少數適當的目標，藉此提高投資報酬率。

已攔截的威脅總數 (2012 年至 2015 上半年)



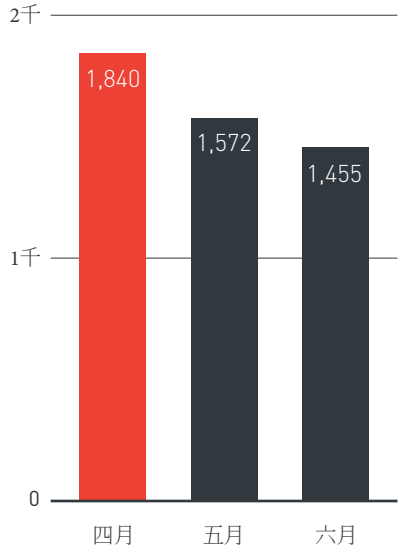
Smart Protection Network 偵測到的威脅數量大致上逐年減少 20%。

已攔截的威脅總數 (2015 年第二季)



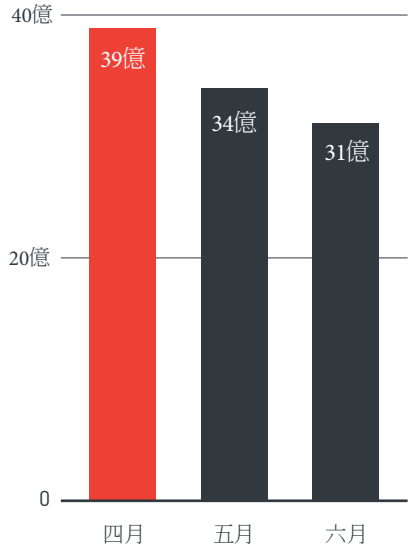
本季，我們每個月平均攔截 42 億個威脅，較上一季的 47 億略為減少。

趨勢科技整體偵測速率：每秒攔截的威脅數量 (2015 年第二季)



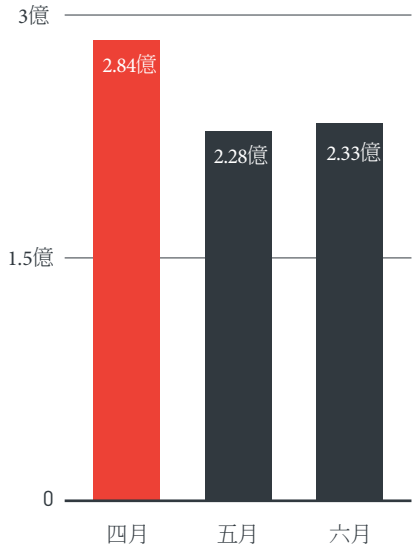
本季，我們平均每秒攔截 1,622 個威脅，較上一季的每秒 1,800 個威脅略低。

被電子郵件信譽評等查詢判定為垃圾郵件的數量 (2015 年第二季)



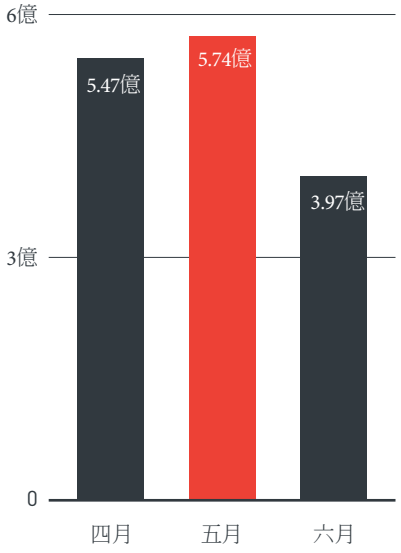
我們總共防止了105 億封來自垃圾郵件散發 IP 位址的電子郵件進入使用者的收件匣當中，較上一季的 120 億封，有顯著的減少。可能的原因之一或許是垃圾郵件散發者慢慢改用其他訊息發送途徑，而非完全單靠電子郵件。

已防止使用者存取惡意網站的次數 (2015 年第二季)



本季，我們防止使用者連上惡意網站的次數超過 7.45 億次，數量從四月到五月略為減少，六月又少許回升。

已攔截的惡意檔案數量 (2015 年第二季)



本季，我們防止了超過 10 億個惡意檔案感染使用者裝置，
惡意程式數量從五月至六月減少了 2.87 億。

已防止使用者存取的惡意網址 (2015 年第二季)

網域	防止存取的原因
sso.anbtr.com	會挾持瀏覽器，危險網站。
cnfg.toolbarservices.com	會挾持瀏覽器，擅自變更使用者瀏覽器的首頁與預設搜尋網站。
jsgnr.eshopcomp.com	在畫面上彈出大量廣告。
initilizeinstall.net	會連上多個散布惡意程式的網站。
sp-storage.spccint.com	惡意程式的幕後通訊網站。
bugreport.yac.mx	與使用者在不知情狀況下連上的惡意網站所下載的 ADW_INCORE 廣告軟體有所關聯。
checkver.dsiteproducts.com	惡意程式的幕後通訊網站。
reports.montiera.com	惡意程式的幕後通訊網站。
creative.ad120m.com	散布惡意和有害的程式。
log.data-url.com	惡意程式和其他有害程式的幕後通訊網站。

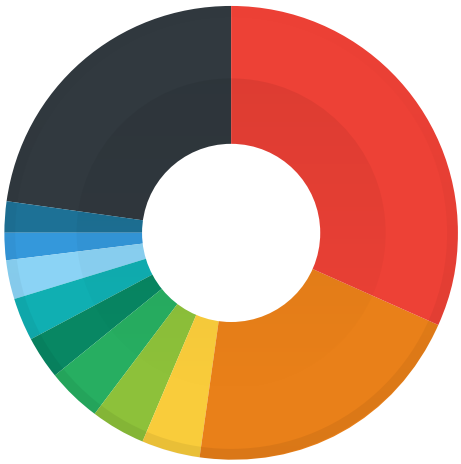
會挾持瀏覽器的網站是存取次數最多的惡意網址。

惡意網址數量最多的國家 (2015 年第二季)

美國	28%
中國	6%
俄羅斯	3%
葡萄牙	3%
荷蘭	2%
德國	2%
英國	2%
南韓	1%
法國	1%
日本	1%
其他	51%

美國依然是惡意網址最多的國家。不過，中國和俄羅斯已將荷蘭擠出前三名之外。

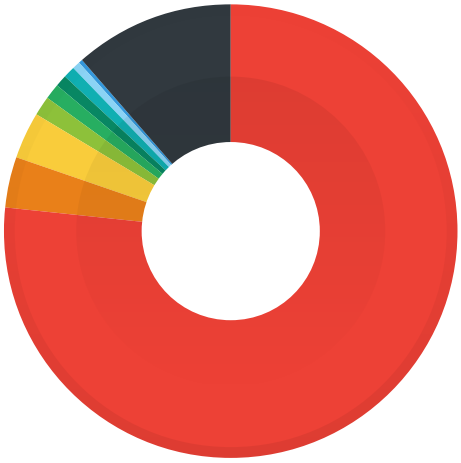
點選惡意網址的使用者數量最多的國家 (2015 年第二季)



美國	32%
日本	21%
台灣	4%
印度	4%
澳洲	4%
德國	3%
中國	3%
加拿大	3%
法國	2%
義大利	2%
其他	22%

點選惡意網址的使用者數量最多的國家在本季沒有太大變化。

垃圾郵件最多的語言 (2015 年第二季)



英文	76.9%
中文	3.7%
德文	3.3%
日文	1.4%
波蘭文	1.0%
西班牙文	0.9%
俄羅斯文	0.8%
葡萄牙文	0.5%
荷蘭文	0.2%
法文	0.2%
其他	11.1%

英文依然是垃圾郵件最多的語言。不過，中文和德文出現的比例較以往多了許多。

散發垃圾郵件最多的國家 (2015 年第二季)

美國	17%
俄羅斯	13%
中國	9%
越南	5%
日本	4%
烏克蘭	3%
印度	3%
西班牙	3%
南韓	2%
巴西	2%
其他	39%

本季散發垃圾郵件最多的國家前三名仍維持不變。

惡意程式家族排行榜 (2015 年第二季)

家族	數量
SALITY	8.8萬
DOWNAD	7.7萬
GAMARUE	5.8 萬
BROWSEVIEW	5.7萬
DUNIHI	4.7萬
UPATRE	4萬
DLOADR	4萬
RAMNIT	3.9萬
VIRUX	3.6萬
ANDROM	2.9萬

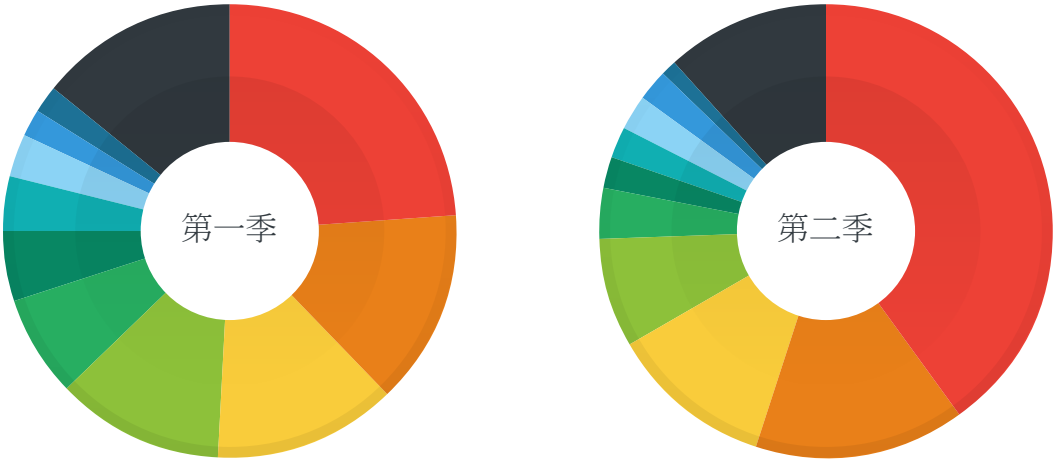
惡意程式家族排行榜 (依市場區隔，2015 年第二季)

市場區隔	識別名稱	數量
大型企業	DOWNAD	5.8萬
	SALITY	3.3萬
	DUNIHI	2.8萬
中小企業	UPATRE	1.2萬
	DLOADR	1.2萬
	DOWNAD	1.1萬
一般消費者	GAMARUE	3.2萬
	SALITY	3.1萬
	VIRUX	1.7萬

本季檔案感染程式 VIRUX 是一般消費者市場前三名的新面孔。VIRUX 會透過可卸除式磁碟和網路共用資料夾散布。

存在已久的銀行惡意程式 EMOTET 過去這一季仍在特定地區相當流行。EMOTET 的偵測數量逐季增加，它們專門誘騙德國使用者點選假冒 DHL 通知電子郵件中的惡意連結。[57]

網路銀行惡意程式家族十大排行榜 (2015 年第一季和第二季)



第一季		第二季	
RAMNIT	24%	RAMNIT	35%
ZBOT	14%	DORKBOT	13%
QAKBOT	13%	ZBOT	13%
DORKBOT	12%	EMOTET	10%
DYRE	7%	DYRE	7%
QBOTCONF	5%	QAKBOT	3%
EMOTET	4%	DRIDEX	2%
BANKER	3%	BANKER	2%
VAWTRAK	2%	FAREIT	2%
URSNIF	2%	BANLOAD	2%
其他	14%	其他	11%

網路銀行頭號惡意程式 RAMNIT 專門竊取敏感資訊，包括電腦上儲存的 FTP 帳號登入資訊以及瀏覽器 Cookie。它基本上是一個檔案感染程式，甚至能感染 HTML 檔案，因此在數量上逐季增加。

越權廣告程式家族排行榜 (2015 年第二季)

家族	數量
OPENCANDY	42.3萬
FAKEGOOG	20.8萬
MYPCBACKUP	16.1萬
ELEX	11.8萬
CROSSRIDER	10萬
DEALPLY	9萬
SPROTECT	8.3萬
MULTIPLUG	8.2萬
TOMOS	7.8萬
ADVSYSTEMPROTECTOR	7.6萬

越權廣告程式家族排行榜 (依市場區隔，2015 年第二季)

市場區隔	識別名稱	數量
大型企業	OPENCANDY	5萬
	FAKEGOOG	1.6萬
	CROSSRIDER	1.5萬
中小企業	OPENCANDY	2萬
	DEALPLY	7千
	FAKEGOOG	7千
一般消費者	OPENCANDY	32.4萬
	FAKEGOOG	16.1萬
	MYPCBACKUP	12.2萬

OPENCANDY 和 MYPCBACKUP 暗藏在一些工具列和其他免費軟體當中。而它們所帶來的彈出式廣告，一般來說是令人討厭的。

Android 惡意程式家族排行榜 (2015 年第二季)

GUIDEAD	24%
SYSSERVICE	10%
SPTVT	10%
FICTUS	5%
SMFORW	4%
SMSREG	3%
FAKEINST	3%
DROPPER	2%
OPFAKE	2%
SYSNOTIFY	1%
其他	35%

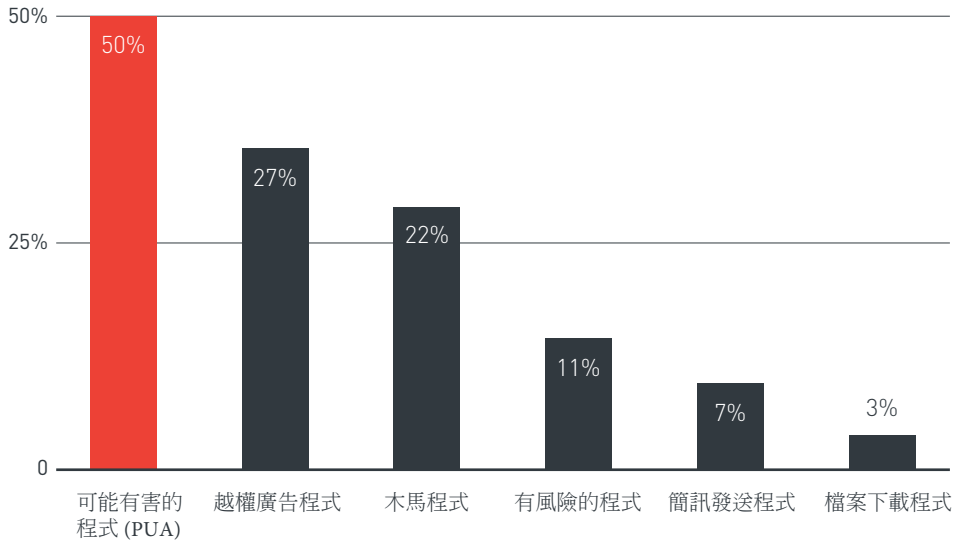
GUIDEAD 變種並無圖形使用者介面 (GUI) 或圖示，安裝之後只會在背後暗中執行。

Android 越權廣告程式家族排行榜 (2015 年第二季)

ADLEAK	13%
ARPUSH	8%
AGENT	7%
IGEXIN	3%
DOWGIN	3%
FLEXLEAK	3%
REVMOB	3%
YOUM	3%
WAPSX	2%
ADS	2%
其他	54%

如同在上一季，ADLEAK 是一個通用名稱，代表可能造成使用者隱私風險的各種應用程式，是過去這一季數量最多的越權廣告程式。

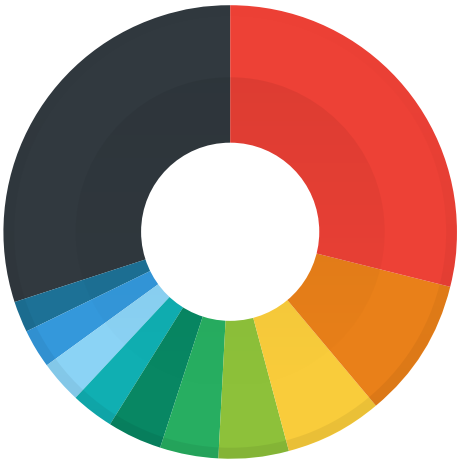
Android 前幾大威脅類型分布比例 (2015 年第二季)



本季出現的 Android 威脅有半數是可能有害的程式 (PUA)。所謂「有風險的程式」(Riskware) 是指擁有某些功能可能被用於惡意用途的程式。

註：某個行動裝置威脅家族可能出現不只一種類型的行為。

C&C 伺服器最多的國家 (2015 年第二季)



美國	29%
烏克蘭	10%
俄羅斯	7%
德國	5%
法國	4%
英國	4%
荷蘭	3%
中國	3%
南韓	3%
波蘭	2%
其他	30%

本季 C&C 伺服器廣泛分散在美國、烏克蘭、俄羅斯等國。請注意，駭客不一定位於這些國家就能控制 C&C 伺服器，因為這些伺服器皆可以從遠端遙控。排行榜中的大部分國家同樣也是惡意網址數量最多的國家，這代表歹徒可能濫用了各種的代管服務和基礎架構。

C&C 伺服器連線數量最多的國家 (2015 年第二季)

美國	38%
印度	12%
日本	7%
土耳其	5%
德國	4%
澳洲	4%
台灣	2%
法國	2%
越南	2%
馬來西亞	2%
其他	22%

美國是 C&C 連線數量最多的國家。

參考資料

1. Evan Perez。(2015 年 5 月 19 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「FBI：駭客宣稱已掌控班機引擎控制系統」(FBI: Hacker Claimed to Have Taken Over Flight's Engine Controls)。上次存取時間 2015 年 7 月 28 日：http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/.
2. Martin Rösler。(2015 年 5 月 19 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「空中駭客：您需要擔心嗎？」(Mile-High Hacking: Should You Worry?)上次存取時間 2015 年 7 月 28 日：http://blog.trendmicro.com/trendlabs-security-intelligence/mile-high-hacking-should-you-worry/.
3. Kim Zetter。(2015 年 5 月 15 日)。*Wired*。「FBI 表示曾遭驅離的研究人員強行控制了一架飛機」(Feds Say That Banned Researcher Commandeered a Plane)。上次存取時間 2015 年 7 月 28 日： http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.
4. BBC。(2015 年 6 月 21 日)。*BBC 新聞*。「波蘭國家航空 (LOT) 班機遭電腦駭客停飛」(Polish LOT Aeroplanes Grounded by Computer Hack)。上次存取時間 2015 年 7 月 28 日： http://www.bbc.com/news/world-europe-33219276.
5. Jaydeep Dave。(2015 年 5 月 20 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「新的路由器攻擊顯示假警告訊息」(New Router Attack Displays Fake Warning Messages)。上次存取時間 2015 年 7 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/new-router-attack-displays-fake-warning-messages/.
6. Fernando Mercês。(2015 年 5 月 28 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「DNS 篡改程式盯上家用路由器」(DNS Changer Malware Sets Sights on Home Routers)。上次存取時間 2015 年 7 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/dns-changer-malware-sets-sights-on-home-routers/.
7. Christopher Budd。(2015 年 4 月 10 日)。*趨勢科技就是要安全部落格 (Simply Security Blog)*。「法國 TV5MONDE 電視台遭到攻擊：改變世界的四個小時」(The TV5MONDE Attack: Four Hours That Changed the World)。上次存取時間 2015 年 7 月 28 日： http://blog.trendmicro.com/the-tv5monde-attack-four-hours-that-changed-the-world/.
8. Lord Alfred Remorin。(2015 年 6 月 25 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「更換供應商詐騙：網路犯罪者如何利用一個 35 美元的惡意程式賺到數百萬美元」(Change of Supplier Fraud: How Cybercriminals Earned Millions Using a $35 Malware)。上次存取時間 2015 年 7 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/change-of-supplier-fraud-how-cybercriminals-earned-millions-using-a-35-malware/.
9. 趨勢科技。(2015 年 5 月 26 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「加拿大網路犯罪個體戶 Frapstar 發動攻擊」(Attack of the Solo Cybercriminals—Frapstar in Canada)。上次存取時間 2015 年 7 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/attack-of-the-solo-cybercriminals-frapstar-in-canada/.
10. 趨勢科技。(2015 年 6 月 30 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Lordfenix：一位利用銀行惡意程式賺錢的 20 歲巴西青年」(Lordfenix: 20-Year-Old Brazilian Makes Profit Off Banking Malware)。上次存取時間 2015 年 7 月 28 日：http://blog.trendmicro.com/trendlabs-security-intelligence/lordfenix-20-year-old-brazilian-makes-profit-off-banking-malware/.
11. 趨勢科技資深威脅研究員。(2015 年 4 月 13 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「單人 PoS 惡意程式行動在巴西竊取了 22,000 筆信用卡資料」(One-Man PoS Malware Operation Captures 22,000 Credit Card Details in Brazil)。上次存取時間 2015 年 7 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-fighting-a-new-pos-malware-family/.
12. Peter Pi。(2015 年 6 月 16 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Magnitude 漏洞攻擊套件利用新修補的 Adobe 漏洞：美國、加拿大、英國遭駭的風險最高」(Magnitude Exploit Kit Uses Newly Patched Adobe Vulnerability; US, Canada, and UK Are Most at Risk)。上次存取時間 2015 年 7 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/magnitude-exploit-kit-uses-newly-patched-adobe-vulnerability-us-canada-and-uk-are-most-at-risk/.
13. Paul Pajares。(2015 年 7 月 1 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「TorrentLocker 在英國的數量暴增，更多社交工程誘餌」(TorrentLocker Surges in the UK, More Social Engineering Lures Seen)。上次存取時間 2015 年 7 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/torrentlocker-surges-in-the-uk-more-social-engineering-lures-seen/.
14. Veo Zhang。(2015 年 6 月 2 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「90 世代駭客：中國青年做起行動勒索軟體生意」(Attack of the 90s Kids: Chinese Teens Take On the Mobile Ransomware Trade)。上次存取時間 2015 年 7 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/attack-of-the-90s-kids-chinese-teens-take-on-the-mobile-ransomware-trade/.
15. TrendLabs。(2015 年 4 月 9 日)。*趨勢科技資訊安全新聞*。「破獲 Beebone 殭屍網路：趨勢科技解決方案」(Beebone Botnet Takedown: Trend Micro Solutions)。上次存取時間 2015 年 7 月 29 日：http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions.

16. Europol。(2015 年 4 月 9 日)。*Europol*。「國際警方鎖定變形的 Beebone 殭屍網路」(International Police Operation Targets Polymorphic Beebone Botnet)。上次存取時間 2015 年 7 月 29 日： https://www.europol.europa.eu/content/international-police-operation-targets-polymorphic-beebone-botnet.
17. US-CERT。(2015 年 4 月 9 日)。*US-CERT*。「警示 (TA15-098A): AAEH」Alert (TA15-098A): AAEH)。上次存取時間 2015 年 7 月 29 日： https://www.us-cert.gov/ncas/alerts/TA15-098A.
18. INTERPOL。(2015 年 4 月 13 日)。*INTERPOL*。「國際刑警組織指揮跨國行動破獲 SIMDA 殭屍網路」(INTERPOL Coordinates Global Operation to Take Down SIMDA Botnet)。上次存取時間 2015 年 7 月 29 日： http://www.interpol.int/News-and-media/News/2015/N2015-038.
19. 趨勢科技。(2015 年 4 月 12 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「SIMDA 殭屍網路遭到破獲」(SIMDA: A Botnet Takedown)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/simda-a-botnet-takedown/.
20. Andy Greenberg。(2015 年 2 月 4 日)。*Wired*。「絲路地下市集首腦 Ross Ulbricht 所有七項罪名皆被判成立」(Silk Road Mastermind Ross Ulbricht Convicted of All 7 Charges)。上次存取時間 2015 年 7 月 29 日： http://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict/.
21. Sam Thielman。(2015 年 5 月 29 日)。*The Guardian*。「絲路經營者 Ross Ulbricht 被判終身監禁」(Silk Road Operator Ross Ulbricht Sentenced to Life in Prison)。上次存取時間 2015 年 7 月 29 日： http://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced.
22. Vincenzo Ciancaglini。(2015 年 6 月 22 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「深入深層全球網路 (Deep Web)」(Digging into the Deep Web)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/digging-into-the-deep-web/.
23. TrendLabs。(2015 年 6 月 5 日)。*趨勢科技資訊安全新聞*。「愛國者法案修訂：對您有何影響？」(The Patriot Act Revision: What Does It Mean to You?) 上次存取時間 2015 年 7 月 29 日： http://www.trendmicro.com/vinfo/us/security/news/online-privacy/patriot-act-revision-underway-what-does-it-mean-to-you.
24. David Sancho。(2015 年 6 月 18 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「美國政府、維基百科皆全面採用 HTTPS：一般網站是否應該跟進？」(US Government, Wikipedia Go All-HTTPS. Should Site Owners Do It, Too?)上次存取時間 2015 年 7 月 29 日：http://blog.trendmicro.com/trendlabs-security-intelligence/us-government-wikipedia-go-all-https-should-site-owners-do-it-too/.
25. Warwick Ashford。(2015 年 6 月 15 日)。*ComputerWeekly.com*。「歐盟資料保護規範將於 2015 年底定案」(EU Data Protection Regulation to Be Finalized by End of 2015)。上次存取時間 2015 年 7 月 29 日： http://www.computerweekly.com/news/4500248164/EU-Data-Protection-Regulation-to-be-finalised-by-end-of-2015.
26. TrendLabs。(2015 年 6 月 5 日)。*趨勢科技資訊安全新聞*。「美國人事管理局 (OPM) 駭客事件洩漏四百萬聯邦員工個資」(US OPM Hack Exposes Data of 4 Million Federal Employees)。上次存取時間 2015 年 7 月 29 日： http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/us-opm-hack-exposes-data-of- 4-million-federal-employees.
27. Ellen Nakashima。(2015 年 7 月 9 日)。*The Washington Post*。「駭客造成美國人事管理局 (OPM) 資料庫外洩，聯邦政府表示有 2,210 萬人受害」(Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say)。上次存取時間 2015 年 7 月 29 日： http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.
28. TrendLabs。(2014 年 9 月 25 日)。*趨勢科技資訊安全新聞*。「鎖定目標攻擊利用跳島式攻擊」(Utilizing Island Hopping in Targeted Attacks)。上次存取時間 2015 年 7 月 29 日： http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/utilizing-island-hopping-in-targeted-attacks.
29. Ashley Carmann。(2015 年 7 月 13 日)。*SC Magazine*。「前白宮網路安全顧問表示，美國人事管理局 (OPM) 外洩的後續效應我們可能永遠都無法完全掌握」(OPM Repercussions Might Never Be Fully Understood, Says Former White House Cybersecurity Advisor)。上次存取時間 2015 年 7 月 31 日： http://www.scmagazine.com/opm-repercussions-might-never-be-fully-understood-says-former-white-house-cybersecurity-advisor/article/426140/.
30. Christopher Budd。(2015 年 5 月 27 日)。*趨勢科技就是要安全部落格 (Simply Security Blog)*。「美國國稅局遭駭：代表的意義和對您的影響」(The IRS Hack: What It Means and What It Means for You)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/the-irs-hack-what-it-means-and-what-it-means-for-you/.
31. Internal Revenue Service。(2015 年 6 月 2 日)。*IRS*。「美國國稅局對於 Get Transcript 應用程式的聲明」(IRS Statement on the 'Get Transcript' Application)。上次存取時間 2015 年 7 月 29 日：http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application.
32. Reuters。(2015 年 6 月 1 日)。*The Asahi Shimbun*。「日本年金系統遭駭，125 萬筆個資外流」(Japan Pension System Hacked, 1.25 Million Cases of Personal Data Leaked)。上次存取時間 2015 年 7 月 31 日： http://ajw.asahi.com/article/behind_news/social_affairs/AJ201506010096.
33. Feike Hacquebord。(2015 年 4 月 16 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Pawn Storm 攻擊活動激增，鎖定北大西洋公約組織 (NATO) 與美國白宮」(Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/.

34. Kervin Alintanahin。(2015 年 5 月)。*趨勢科技資訊安全情報*。「Tropic Trooper 攻擊行動：利用長期驗證的舊漏洞來滲透您的機密單位」(Operation Tropic Trooper: Relying on Tried-and-Tested Flaws to Infiltrate Secret Keepers)。上次存取時間 2015 年 7 月 29 日： http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf.
35. TrendLabs。(2015 年 5 月 14 日)。*趨勢科技資訊安全新聞*。「Tropic Trooper 攻擊行動如何滲透您的機密單位」(How Operation Tropic Trooper Infiltrates Secret Keepers)。上次存取時間 2015 年 7 月 29 日： http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-tropic-trooper-infiltrates-secret-keepers.
36. Robert Abel。(2015 年 6 月 17 日)。*SC Magazine*。「Lotus Blossom 網路攻擊行動襲擊東南亞軍事及政府單位」(Lotus Blossom' Cyber Attacks Hit Military, Government Targets in Southeast Asia)。上次存取時間 2015 年 7 月 29 日： http://www.scmagazine.com/researchers-discover-50-cyber-attacks-in-lotus-blossom-campaign/article/421279/.
37. Ming Yen Hsieh。(2015 年 6 月 26 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「ESILE/Lotus Blossom 攻擊行動現況」(The State of the ESILE/Lotus Blossom Campaign)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/the-state-of-the-esilelotus-blossom-campaign/.
38. Karl Dominquez。(2011 年 19 月 10 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「密切監控下一個 STUXNET」(Keeping Tabs on the Next STUXNET)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/keeping-tabs-on-the-next-stuxnet/.
39. Jack Tang。(2015 年 6 月 17 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「CVE-2015-2360分析：DUQU 2.0 零時差漏洞」(Analysis of CVE-2015-2360—DUQU 2.0 Zero-Day Vulnerability)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/analysis-of-cve- 2015-2360-duqu-2-0-zero-day-vulnerability/ .
40. Samuel Gibbs。(2015 年 6 月 11 日)。*The Guardian*。「DUQU 2.0：伊朗核武談判會場發現『涉及以色列』的電腦病毒」(DUQU 2.0: Computer Virus 'Linked to Israel' Found at Iran Nuclear Talks Venue)。上次存取時間 2015 年 7 月 29 日： http://www.theguardian.com/technology/2015/jun/11/duqu-20-computer-virus-with-traces-of-israeli-code-was-used-to-hack-iran-talks.
41. Jay Yaneza。(2015 年 5 月 4 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「巨集惡意程式：老技倆依舊有效 -- 第一篇」(Macro Malware: When Old Tricks Still Work, Part 1)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/macro-malware-when-old-tricks-still-work-part-1/.
42. Jay Yaneza。(2015 年 5 月 7 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「巨集惡意程式：老技倆依舊有效 -- 第二篇」(Macro Malware: When Old Tricks Still Work, Part 2)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/macro-malware-when-old-tricks-still-work-part-2/.
43. TrendLabs。(2015 年 7 月 1 日)。*趨勢科技資訊安全新聞*。「eBay 採用的 Magento 電子商務平台遭到支付卡竊盜集團駭入」(eBay's Magento E-Commerce Platform Hit by Payment Card Stealers)。上次存取時間 2015 年 7 月 31 日： http://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/ebay-magento-ecommerce-platform-hit-by-payment-card-stealers.
44. Charlie Osborne。(2015 年 6 月 22 日)。*ZDNet*。「eBay 修補 Magento 電子商務平台的輸入、XSS 及 CSRF 漏洞」(eBay Patches Input, XSS, CSRF Vulnerabilities in Magento E-Commerce Platform)。上次存取時間 2015 年 7 月 31 日： http://www.zdnet.com/article/ebay-patches-input-xss-csrf-vulnerabilities-in-magento-e-commerce-platform/.
45. Jaydeep Dave。(2015 年 4 月 29 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「WordPress 漏洞讓數百萬網站陷入危險：趨勢科技有解」(WordPress Vulnerability Puts Millions of Sites at Risk; Trend Micro Solutions Available)。上次存取時間 2015 年 7 月 31 日： http://blog.trendmicro.com/trendlabs-security-intelligence/wordpress-vulnerability-puts-millions-of-sites-at-risk-trend-micro-solutions-available/.
46. NowSecure, Inc. (2015 年)。*NowSecure*。「Samsung 手機鍵盤安全漏洞：全球超過 6 億台裝置受到影響」(Samsung Keyboard Security Risk Disclosed: Over 600M+ Devices Worldwide Impacted)。上次存取時間 2015 年 7 月 31 日： https://www.nowsecure.com/keyboard-vulnerability/.
47. The MITRE Corporation。(2015 年)。*CVE*。「CVE-2015-4640」。上次存取時間 2015 年 7 月 31 日： http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4640.
48. The MITRE Corporation。(2015 年)。*CVE*。「CVE-2015-4641」。上次存取時間 2015 年 7 月 31 日： http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4641.
49. 趨勢科技。(2015 年 6 月 19 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Samsung SwiftKey 漏洞：您該知道的事與如何自保」(The Samsung SwiftKey Vulnerability—What You Need to Know and How to Protect Yourself)。上次存取時間 2015 年 7 月 31 日： http://blog.trendmicro.com/trendlabs-security-intelligence/the-samsung-swiftkey-vulnerability-what-you-need-to-know-and-how-to-protect-yourself/.

50. Christopher Budd。(2015 年 6 月 18 日)。*趨勢科技就是要安全部落格 (Simply Security Blog)*。「無法修補的 Android 裝置？」(Unpatchable Android?) 上次存取時間 2015 年 7 月 31 日： http://blog.trendmicro.com/unpatchable-android/.
51. Seven Shen。(2015 年 5 月 27 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「趨勢科技發現可讓歹徒單鍵篡改 Android App 程式的 Apache Cordova 漏洞」(Trend Micro Discovers Apache Cordova Vulnerability that Allows One-Click Modification of Android Apps)。上次存取時間 2015 年 7 月 31 日： http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-apache-vulnerability-that-allows-one-click-modification-of-android-apps/.
52. The MITRE Corporation。(2015 年)。*CVE*。「CVE-2015-1835」。上次存取時間 2015 年 7 月 31 日： https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1835.
53. Dan Goodin。(2015 年 6 月 18 日)。*Ars Technica*。「嚴重的 OS X 和 iOS 漏洞能讓駭客竊取鑰匙圈和 1Password 資料」(Serious OS X and iOS Flaws Let Hackers Steal Keychain, 1Password Contents)。上次存取時間 2015 年 7 月 31 日： http://arstechnica.com/security/2015/06/serious-os-x-and-ios-flaws-let-hackers-steal-keychain-1password-contents/.
54. The MITRE Corporation。(2015 年)。*CVE*。「CVE-2015-1671」。上次存取時間 2015 年 8 月 5 日： http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1671.
55. Brooks Li。(2015 年 7 月 7 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Hacking Team 的 Flash 零時差漏洞攻擊已被收錄到漏洞攻擊套件當中」(Hacking Team Flash Zero-Day Integrated Into Exploit Kits)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/.
56. Peter Pi。(2015 年 7 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Hacking Team 資料外洩事件又一個零時差漏洞曝光」(Another Zero-Day Vulnerability Arises from Hacking Team Data Leak)。上次存取時間 2015 年 7 月 29 日： http://blog.trendmicro.com/trendlabs-security-intelligence/another-zero-day-vulnerability-arises-from-hacking-team-data-leak/.
57. Michael Angelo Casayuran。(2015 年 5 月 19 日)。*趨勢科技威脅百科 (Threat Encyclopedia)*。「假冒 DHL 的垃圾郵件暗藏 EMOTET」(DHL Spam Arrives with EMOTET)。上次存取時間 2015 年 8 月 4 日： http://www.trendmicro.com/vinfo/us/threat-encyclopedia/spam/3561/dhl-spam-arrives-with-emotet.

作者：
TrendLabs
趨勢科技全球技術支援與研發中心

趨勢科技

趨勢科技是全球雲端安全領導廠商，致力為企業和消費者開發網際網路內容安全與威脅管理解決方案，建立一個安全的數位資訊交流世界。身為伺服器安全的先驅，擁有 20 多年經驗，我們專門提供符合客戶及合作夥伴需求的頂尖用戶端、伺服器及雲端安全防護，更快攔截新的威脅，保護實體、虛擬及雲端環境內的資料。我們領先業界的雲端運算防護技術、產品及服務皆以趨勢科技 Smart Protection Network™ 基礎架構為後盾，能在威脅出現的來源，也就是網際網路，直接攔截威脅，並且還有全球 1,000 多位威脅情報專家在背後支援。如需更多資訊，請至：www.trendmicro.tw

TREND MICRO™

Securing Your Journey to the Cloud

©2015 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro 與 t 字球形標誌是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為各該公司的商標或註冊商標。